耐タンパー性低遅延暗号ハードウェアに関する研究

博士学位論文要約（平成31年３月）

耐タンパー性低遅延暗号ハードウェアに関する研究

ヴィッレ　ウリマウル
指導教員：青木　孝文

Tamper-Resistant Low-Latency Cryptographic Hardware

Ville YLI-MÄYRY
Supervisor: Takafumi AOKI

Cryptography is an important field in the increasingly interconnected world. In recent years, design of lightweight cryptography has become more popular. Lightweight cryptography is concerned with designing cryptographic modules that can operate in environments with restricted computing resources, such as limited program size, memory, or processing power, for example. Lightweight hardware ciphers have developed two main design goals. First, to design as small as possible modules, and second to have low latency from data input to data output. In particular, lightweight ciphers with an ultra-low latency, capable of encryption/decryption in a single clock cycle, have gained momentum in the last few years. They've shown that very low latency encryption/decryption is possible with modest costs in comparison with traditional round-based designs. On the other hand, the implementation security of cryptographic modules has also been a strongly research field in the last years. Implementation security deals with the physical characteristics of the implementation and their relation to the information security of the device. This thesis explores what kinds of threats one aspect of implementation security, namely side-channel analysis, poses against low latency cryptographic hardware. We explore existing side-channel analysis methods against low latency cryptographic modules, and show a new point of potential information leakage and how to exploit it. Further, we demonstrate these points experimentally in a real-world setting on Field Programmable Gate Array (FPGA) and Application Specific Integrated Circuit (ASIC) hardware platforms. Finally, we propose a new variant of an anti-tamper countermeasure suited specifically for these type of low latency ciphers.

1. Introduction

Interest in lightweight cryptography has increased greatly as the need for encryption of communication between resource-restricted embedded devices has grown. With advances in semiconductor technology, embedded devices are being pushed to ever smaller size, and many new possibilities in applications can be expected with interconnected embedded device communication. In new models of networking, embedded devices connect to each other and may form ad-hoc networks, exchanging information and controlling each other. Each device then requires the capability to communicate, and, as a direct result, the capability for cryptographic processing to ensure secure communication. In the past however, cryptographic algorithms have mainly been designed firstly from a security point of view to make sure that they are robust against mathematical cryptanalysis. As a result, designs generally did not take into consideration the power consumption or other resources limited in embedded devices. To solve these types of challenges with available resources, recent lightweight cipher design propositions aim to be efficient with respect to circuit or program size, power consumption, memory requirements etc. while still sustaining the required level of mathematical security. The standardization of such ciphers has already begun with ISO/IEC29192-2, and a great number of lightweight ciphers have been introduced for use in environments with strictly limited resources. One interesting direction in lightweight ciphers is the design of low latency ciphers. In addition to being resource efficient, these type of ciphers main goal is to process the input data with as little latency as possible. For achieving lower latency processing is generally performed in one clock cycle. Such and implementation technique is called unrolling or unfolding, and the corresponding hardware is called an unrolled or an unfolded architecture. In this work, we focus on this type of unrolled ciphers.

2. Unrolled Implementation and Side-Channel Attacks

A distinguishing character in power consumption in ciphers with an unrolled architecture is that since no

Table 1: Implementation cost for Unrolled TI and the proposed countermeasure

Unrolled TI	Area	Delay	Protected rounds
w/o countermeasure	8512 GE	9 ns	Unprotected
w/ countermeasure	48012 GE	13.2 ns	Rounds 1 and 10

This work	Area	Delay	Protected rounds
w/o countermeasure	9647 GE	5.46 ns	Unprotected
w/ countermeasure	59765 GE	7.09 + t_{dg} ns	Rounds 1-4

memory elements, that is registers, are used, the power consumption of a cipher implemented in this manner consists mainly of gate switching that takes place inside the circuit as the cipher's functions are being evaluated. Because the whole cipher is in effect a large combinatorial circuit, the power consumption of an encryption or decryption operation in the cipher depends on two consecutive inputs. During an encryption or decryption operation, power consumption takes place when the combinatorial circuit changes from the state it was left by the last input before, to the state caused by the new input data. Consequently, two identical inputs will produce near zero power consumption, because the internal state of the circuit does not change between the first and second plaintext. Further, this reasoning can be extended to partially equal plaintexts: bits where the plaintexts are equal will not contribute to the switching in the circuit in the parts of the circuit that depend won those bits.

3. Experiments

We show through experiments with FPGA and ASIC implementations of a low-latency block cipher called PRINCE[1] firstly, attacks in the literature against traditional block ciphers and how they can be applied to unrolled architectures, and secondly, discuss the special properties of unrolled architectures which make possible other types of attacks. We show that the secret key used during encryption and decryption processing can be retrieved by an attacker that can observe power consumption in the cryptographic device with Correlation Power Analysis [2]. Against these attacks, we propose in the next chapter a new countermeasure for unrolled architectures.

4. Side-Channel Analysis Countermeasures for Unrolled Architectures

Though numerous countermeasures [4] against side-channel attacks have been proposed in the past, they generally are applicable only to ciphers that use registers to hold intermediate values during the processing. For unrolled architectures, there has been one proposal based on a Threshold Implementation (TI) [3]. This design, however, was deemed to be unsecure against side-channel analysis. We present the first masking-based countermeasure suitable for unrolled architecture of low-latency ciphers, named Unrolled Rotating S-boxes Masking (URSM), which is a modified version of Rotating S-boxes Masking (RSM) [6]. RSM is a kind of
lightweight masking method for block ciphers. The main idea of RSM is to transform (i.e., mask) the computation of S-boxes and linear functions into a look-up table, generated by pre-computing the values. The implementation cost and comparison with existing works for the countermeasure is shown in Table 1. The hardware architecture used in shown in Fig. 2. To demonstrate the effectiveness of our proposed implementation, we conduct experiments using an FPGA implementation of the proposed countermeasure design. We evaluate our proposed design with two statistical metrics: t-test as proposed in [5], and the

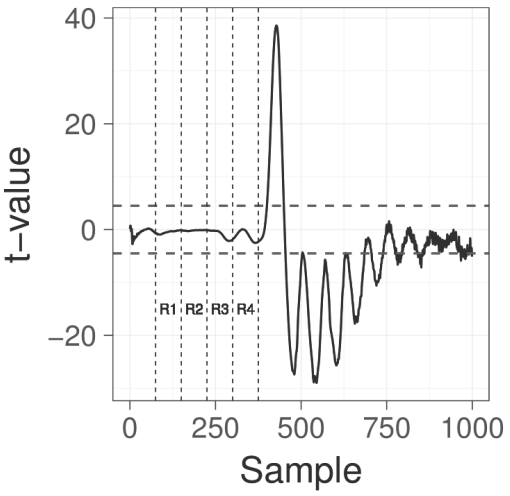

Figure 1: T-test results for the proposed countermeasure

proposed attack presented in the previous section. Fig. 1 shows the t-test results for the proposed design. T-test is a widely used method for assessing the side-channel security of software and hardware implementations of ciphers. We conduct the fixed vs. random test for our design. The results show that in the functions we implemented our countermeasure for the side-channel leakage is suppressed. Further, we test the security of the proposed design by applying the conventional power analysis attacks against our design. The results of the attack are shown in Fig. 2. The horizontal axis shows the amount of power consumption traces used for the attack and the vertical axis shows the corresponding correlation coefficients. Results show that the power analysis was not able to recover secret key information.

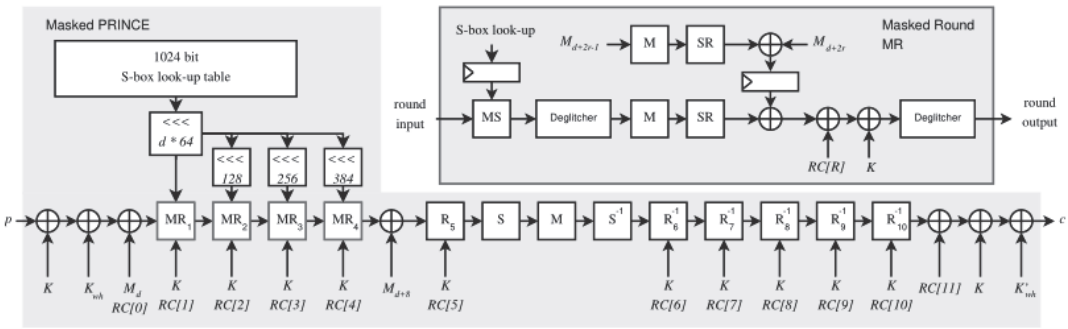

Figure 2: Proposed architecture for masking PRINCE's rounds 1-4

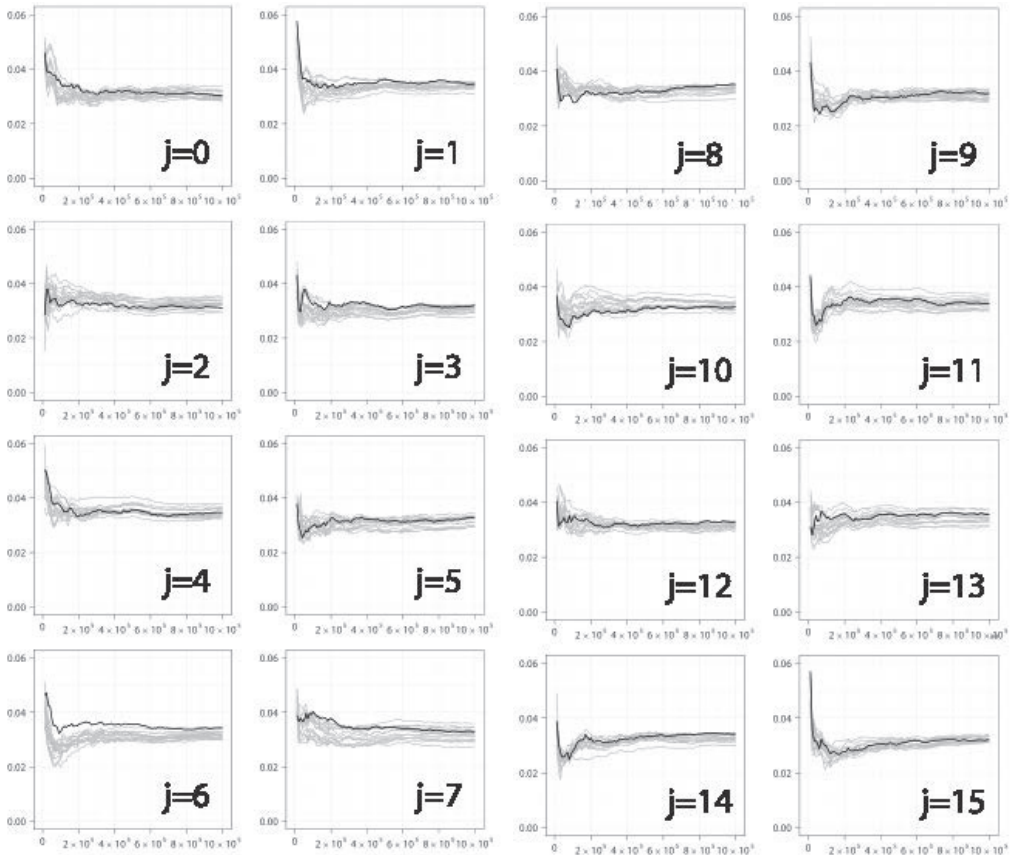

Figure 3: Result of Correlation Power Analysis [2] against the proposed implementation with countermeasure

5. Conclusion

In this thesis, we discussed side-channel leakage in the context of unrolled architectures. We demonstrated how implementations with an unrolled architecture differ from those with a looped architecture, and how side-channel leakage is generated in unrolled architectures. Finally, we proposed a hypothesis how in unrolled architectures, the diffusion characteristics of the cipher can produce side-channel leakage in the inner rounds of the cipher. In general, side-channel leakage related to the first round computation was thought to be exploitable only during the computation of the first round. We demonstrated, however, that first round S-box output differences can produce biases in the switching of the latter rounds, which is correlated with the Hamming distance of the first round S-box, and can perhaps be exploited in a side-channel attack. We demonstrated side-channel attacks on the fully unrolled implementation of PRINCE. We showed that PRINCE is vulnerable to traditional Correlation Power Analysis, even though it is generally though that fully unrolled implementations are somewhat resistant against this type of attack. We showed the ways an attacker can leverage the implementation details to recover the key: either attacking the first and second rounds of the cipher, or using power consumption traces of both encryption and decryption operations in the attack. Secondly, we demonstrated through experiments that the inner rounds of ciphers implemented with unrolled architectures contain side-channel leakage related to the first round S-box function, from which key material can be deduced. Finally, we proposed Unrolled Rotating S-boxes Masking, or U-RSM, a new implementation variation of a countermeasure against side-channel analysis on unrolled implementation of PRINCE. We demonstrated that the countermeasure is implementable effectively in hardware. The countermeasure's area requirements are very competitive with the countermeasures currently in literature. We demonstrated that a PRINCE implementation with U-RSM applied to the first 4 rounds comes with a hardware cost overhead with required area 619% that of the unprotected design, and critical delay 129% that of the unprotected design, not including area/delay overhead of deglitchers. In the countermeasure in literature [3], the respective overheads were 564% in area and 147% in delay. However, the existing countermeasure only protected PRINCE's first and last rounds, which leaves the implementation exposed to the attack on the inner round. We thus showed the first countermeasure for a cipher implemented with a fully unrolled architecture that counters also covers the vulnerable inner rounds. We showed that the countermeasure is valid through two experiments: first, performing a conventional side-channel attack, and showing that key material can not be recovered, and further a statistical method in the literature, based on Welch's t-test.

References

1) J. Borghoff et al. “PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications”. In: Advances in Cryptology – ASIACRYPT 2012. Ed. by Xiaoyun Wang and Kazue Sako. Vol. 7658. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2012, pp. 208–225.
2) E. Brier, Christophe Clavier, F. Olivier. “Correlation Power Analysis with a Leakage Model”. In: Cryptographic Hardware and Embedded Systems - CHES 2004. Ed. by Marc Joye and Jean-Jacques Quisquater. Vol. 3156. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2004, pp. 16–29.
3) A. Moradi and T. Schneider. “Side-Channel Analysis Protection and Low-Latency in Action - case study of PRINCE and Midori”. In: ASIACRYPT. 2016, pp. 517–547.
4) Svetla Nikova, Vincent Rijmen, and Martin Schläffer. “Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches”. In: Journal of Cryptology 24 (2 2011), pp. 292–321.
5) Tobias Schneider and Amir Moradi. “Leakage assessment methodology”. In: Journal of Cryptographic Engineering 6 (2016), pp. 85–99.